Mr. Chairman, thank you for the opportunity to testify about the Department of Justice's views on encryption, and particularly the proposed Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act, introduced by you as S. 798. As you are aware, encryption, and specifically export controls on encryption, presents complex and difficult issues that we are attempting to address with our colleagues throughout the Administration. In my testimony, I will first outline the basic perspective and recent initiatives of the Department of Justice on encryption issues, and will then discuss some specific concerns with the PROTECT Act.

Encryption, the Law Enforcement Perspective

The Department of Justice supports the spread of strong, recoverable encryption. Law enforcement's responsibilities and concerns include protecting privacy and commerce over our nation's communications networks. For example, we prosecute under existing laws those who violate the privacy of others by illegal eavesdropping, computer hacking or theft of confidential information. Over the last few years, the Department has continually pressed for laws protecting confidential information and the privacy of citizens. Furthermore, we help protect commerce by enforcing the laws, including those that protect intellectual property rights, and that combat computer and communications fraud. (In particular, we help to protect the confidentiality of business data through enforcement of the recently enacted Economic Espionage Act.) Our support for robust encryption is a natural outgrowth of our commitment to protecting privacy for personal and commercial interests. As the head of the Criminal Division of the Department of Justice, I hold these values dear.

But the Department of Justice protects more than just privacy. We also protect public safety and national security against the threats posed by terrorists, organized crime, foreign intelligence agents, and others. Moreover, we have the

responsibility for preventing, investigating, and prosecuting serious criminal and terrorist acts when they are directed against the United States. We are gravely concerned that the proliferation and use of non-recoverable encryption by criminal elements would seriously undermine these duties to protect the American people. Therefore, we favor the spread of strong encryption products that permit timely and legal law enforcement access to plaintext.

The most easily understood example is electronic surveillance. Court-authorized wiretaps have proven to be one of the most successful law enforcement tools in preventing and prosecuting serious crimes, including drug trafficking and terrorism. We have used legal wiretaps to bring down entire narcotics trafficking organizations, to rescue young children kidnaped and held hostage, and to assist in a variety of matters affecting our public safety and national security. In addition, as society becomes more proficient in its use of computers, evidence of crimes is increasingly found in stored computer data, which can be searched and seized pursuant to court-authorized warrants. But if non-recoverable encryption proliferates, these critical law enforcement tools would be nullified. Thus, for example, even if the government satisfies the rigorous legal and procedural requirements for obtaining a wiretap order, the wiretap would be worthless if the intercepted communications of the targeted criminals amount to an unintelligible jumble of noises or symbols. Or we might legally seize the computer of a terrorist and be unable to read the data identifying his or her targets, plans and co-conspirators. The potential harm to public safety, law enforcement, and to the nation's domestic security could be devastating.

I want to emphasize that this concern is not theoretical, nor is it exaggerated. Although use of encryption is far from universal, we have already begun to encounter its harmful effects. For example, in an investigation of a multinational child pornography ring, investigators discovered sophisticated encryption used to

conceal thousands of images of child pornography that were exchanged among members. Similarly, in several major computer hacker cases, the subjects have encrypted computer files, thereby concealing evidence of serious crimes. In one such case, the government was unable to determine the full scope of the hacker's activity because of the use of encryption. Finally, criminal use of encryption is becoming increasingly international — the United Kingdom recently reported that in 1996 it seized encrypted files from a Northern Irish terrorist group concerning terrorist targets such as police officers and politicians. In that case, law enforcement was able to read the data, but only after considerable effort.

The lessons learned from these investigations are clear: criminals are beginning to learn that encryption is a powerful tool for keeping their crimes from coming to light. Moreover, as encryption proliferates and becomes an ordinary component of mass market items, and as the strength of encryption products increases, the threat to public safety will increase proportionately.

Given both the benefits presented and risks posed by encryption, the Department believes that encouraging the use of recoverable encryption products — which protect business and personal data as well as public safety — is an important part of the Administration's balanced encryption policy. Recoverable products also fulfill business needs. Information technology companies have told us that their customers recognize the need to ensure recoverability of their data when using strong encryption; otherwise, they risk losing access to their data forever. For example, a company might find that one of its employees lost his encryption key, thus accidentally depriving the business of important and time-sensitive business data. We should point out that loss of an encryption key is not theoretical. One company told us that employees commonly lose or forget their passwords, which must then be restored by system administrators. The same capability must exist for encryption systems. Similarly, a business may find that a disgruntled employee has

encrypted confidential information and then absconded with the key. In these cases, a plaintext recovery system promotes important private sector interests. Indeed, as the Government implements encryption in our own information technology systems, it also has a business need for plaintext recovery to assure that data and information that we are statutorily required to maintain are in fact available at all times. For these reasons, as well as to protect public safety, the Department has been affirmatively encouraging the voluntary development of "plaintext" recovery products, recognizing that only their ubiquitous use will provide both protection for data and protection of public safety. We also want to underscore that in most recoverable systems, businesses will manage their own keys.

Because we remain concerned with the impact of encryption on the ability of law enforcement at all levels of government to protect the public safety, the Department and the FBI are engaged in continuing discussions with industry in a number of different fora. These ongoing, productive discussions seek to find creative solutions, in addition to key recovery, to the dual needs for strong encryption to protect privacy and plaintext recovery to protect public safety and business interests. While we still have work to do, these dialogues have been useful because we have discovered areas of agreement and consensus, and have found promising areas for seeking compromise solutions to these difficult issues. While we do not think that there is one magic technology or solution to all the needs of industry, private citizens, and law enforcement, we believe that by working with those in industry who create and market encryption products, we can benefit from the accumulated expertise of industry to gain a better understanding of technology trends and develop advanced tools that balance privacy and security.

Furthermore, we believe that a constructive dialogue on these issues is the best way to make progress, rather than export control legislation. Although export controls on encryption products have been in place for years and exist primarily to

protect national security and foreign policy interests, they are in no sense inflexible, and have been updated in recent years in a continuing effort to balance the needs of privacy, electronic commerce, public safety, and national security. Indeed, largely as a result of the dialogue the Administration has had with industry, significant progress has been made on export controls. Recent updates were announced by Vice President Gore on September 16, 1998, and implemented in an interim rule, which was issued on December 31, 1998. The Department of Justice supports these updates to export controls, which permit the export of products that have a bit length of 56-bits or less, and also permit the easy export of unlimited-strength encryption to certain industry sectors, including medical facilities and banks, financial institutions, and insurance companies in most jurisdictions. These changes allow these sectors, which possess large amounts of highly sensitive and personal information, to use products that will protect the privacy of their clients. The Administration also expanded its policy to permit recoverable exports, such as encryption systems managed by network administrators, to foreign commercial firms. We learned about these systems through our dialogue with industry. According to industry, such systems are demanded by the market today and are in use. They are also largely consistent with the needs of law enforcement.

The Department, in conjunction with the rest of the Administration, intends to continue our dialogue with industry, and will evaluate the export control process on an ongoing basis in order to ensure that the balance of interests remains fair to all concerned. We agree that there are a wide range of national interests that must be supported, including U.S. industry competitiveness. Hence, we are committed to continued review and dialogue with industry.

At the same time, we must recognize that market forces will only take us so far. To the extent that criminal activity, such as terrorism or child pornography,

occurs outside the business environment, criminals would rather lose data than have it seized by law enforcement. Thus, more must be done. Therefore, the Department of Justice is also trying to address the threat to public safety from the widespread use of encryption by enhancing the ability of the Federal Bureau of Investigation and other law enforcement entities to obtain the plaintext of encrypted communications. Among the initiatives is the funding of a centralized technical resource within the FBI. This resource, when fully established, will support federal, state, and local law enforcement in developing a broad range of expertise, technologies, tools, and techniques to respond directly to the threat to public safety posed by the widespread use of encryption by criminals and terrorists. It will also allow law enforcement to stay abreast of rapid changes in technology. Finally, it will enhance the ability of law enforcement to fully execute the wiretap orders, search warrants, and other lawful process issued by courts to obtain evidence in criminal investigations when encryption is encountered. However, we must recognize that these efforts — while critical — do not (like market forces) alone provide an adequate solution to the encryption problem, as the widespread use of non-recoverable encryption by criminals would quickly overwhelm any possible law enforcement technical response.

The PROTECT Act

In light of the above, the proposed Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act raises several concerns from the perspective of the Department of Justice. First, the Act may impede the voluntary development of products that could assist law enforcement in obtaining access to plaintext. The Administration believes that the development of such products is important for a safe society. For example, the Act might preclude the United States government from utilizing useful and appropriate incentives to develop or use key recovery techniques, such as purchasing key recovery products for its own use and supporting

pilot projects that demonstrate the viability of key recovery.

Second, the Act also could impair the government's ability to engage in secure electronic commerce. We are concerned that the breadth of the language in subsection 202(c) may limit the ability of an agency to require a certain type of authentication mechanism for transactions between the public and the government. (For example, in the context of an electronic filing of a regulatory report, a tax return, or an application for benefits, authentication of the filer's identity is critical, including for any subsequent enforcement action.) This concern is raised because the definition of "encryption" includes the use of mathematical formulas to preserve not only confidentiality, but also integrity or authenticity.

Third, the PROTECT Act places responsibility for developing techniques for obtaining lawful access to the plaintext of communications and data in the National Institute for Standards and Technology (NIST). As I noted above, the Department of Justice has already begun to create a centralized technical resource within the FBI to develop a broad range of expertise, technologies, tools, and techniques to respond to the use of encryption by criminals and terrorists. In my view, the responsibility for developing such tools and techniques should in this case lie with law enforcement, because it is law enforcement that has the operational expertise to understand the requirements for such tools and techniques to be effective. Moreover, it is law enforcement that will actually have to put the techniques into practice. Instead of conferring this new responsibility on NIST, I would request that Congress continue to support our efforts to develop technical expertise within the law enforcement community.

Fourth, we share the deep concern of the National Security Agency that the proposed PROTECT Act would harm national security and public safety interests through the liberalization of export controls far beyond our current policy. Among other decontrols, the proposed Act provides that a product is to be exportable if a

product of equivalent strength or key length *will be* available outside the United States in the next 12 months — even if the product of supposedly equivalent strength is intended for different uses, is not user-friendly or widely used, is not cost-competitive, or does not present the same threats to national security. We are concerned that this considerable decontrol of robust encryption will cause in the near term the easy acquisition of robust encryption products by terrorist organizations and international criminals and frustrate the ability of law enforcement to combat these problems internationally. Moreover, the structure and functions of the proposed Encryption Export Advisory Board raise concerns under separation of powers principles and the Appointments Clause.

It is also important to consider that our allies concur that unrestricted export of encryption poses a significant risk to national security, especially to regions of concern. As recently as December 1998, the thirty-three members of the Wassenaar Arrangement reaffirmed the importance of export controls on encryption for national security and public safety purposes and adopted agreements to enable governments to review exports of hardware and software with a 56-bit key length and above and mass-market products above 64 bits, consistent with national export control procedures. Thus, the elimination of U.S. export controls, as provided by the proposed Act, would severely hamper the international community's efforts to combat such international public safety concerns as terrorism, narcotics trafficking, and organized crime.

In light of these factors, we believe that the Administration's more cautious balanced approach is the best way to protect our commercial interests, including our interest in ensuring the success of U.S. industry and electronic commerce, while simultaneously protecting law enforcement and national security interests. We believe that legislation that eliminates or substantially reduces export controls on encryption could upset that delicate balance and is unwise.

The recent decision of the United States Court of Appeals for the Ninth Circuit in Daniel Bernstein v. United States Department of Justice and United States Department of Commerce has not changed our view that legislation eliminating or substantially reducing export controls is contrary to our national interests. The Department of Commerce and the Department of Justice are currently reviewing the Ninth Circuit's decision in Daniel Bernstein v. United States Department of Justice and United States Department of Commerce, and we are considering possible avenues for further review, including seeking a rehearing of the appeal en banc in the Ninth Circuit. In the interim, the regulations controlling the export of encryption products remain in full effect, even as to Professor Bernstein's own software.

In sum, we as government leaders should embark upon the course of action that best preserves the balance long ago set by the Framers of the Constitution, preserving both individual privacy and society's interest in effective law enforcement. We should promote encryption products which contain robust cryptography but that also provide for timely and legal law enforcement access to encrypted evidence of criminal activity. We should also find ways to support secure electronic commerce while minimizing risk to national security and public safety. This is the Administration's approach. We look forward to working with this Committee as it enters the markup phase of this bill.